ABSTRACT

Authentication method for authenticating a mobile node to a packet data network, in which a shared secret for both the mobile node and the packet data network is arranged by using a shared secret of the mobile node and a telecommunications network authentication centre. In the method, the mobile node sends its subscriber identity to the packet data network together with a replay attack protector. The packet data network obtains authentication triplets, forms a session key using them, and sends back to the mobile node challenges and a cryptographic authenticator made by using the session key. The mobile node can then form the rest of the authentication triplets using the challenges and then form the session key. With the session key, the mobile node can check the validity of the cryptographic authenticator. If the authenticator is correct, the mobile node sends a cryptographic response formed using the session key to the packet data network for authenticating itself to the packet data network.